What is claimed is:

1. A security document comprising:

a substrate;

a first graphic carried by the substrate, the first graphic conveying a photographic image to human viewers thereof,

the first graphic being steganographically encoded to convey first plural bits of data recoverable by computer analysis of said first graphic; and

a second graphic carried by the substrate, the second graphic conveying a visual image to human viewers thereof,

wherein the second graphic is steganographically encoded to convey second plural bits of data recoverable by computer analysis of said second graphic; and

wherein the steganographically encoded first plural bits of data and the steganographically encoded second plural bits of data cooperate to evidence authenticity of the security document.

2. The document of claim 1 wherein the second graphic comprises at least one of a background pattern, a background tint, an image, a graphic design, a photographic image, line-art, a government seal and an artistic design.

3. The document of claim 2 further comprising text printed on the substrate.

4. The document of claim 3 wherein said first plural bits of data and said second plural bits of data each correspond to at least a part of said printed text.

5. The document of claim 1 wherein at least one of said first plural bits of data and said second plural bits of data serves as an index into a registry containing additional information.

6. The document of claim 5 wherein the additional information comprises at least one of a photograph corresponding to the first graphic, biometric information related to a person depicted in the first graphic, and insurance coverage information.

7. The document of claim 1 wherein said steganographic encoding does not visibly interrupt said first or second graphic.

8. The document of claim 1 further comprising steganographic encoding to convey third plural bits, wherein the third plural bits are designed to be lost or to predictably degrade when subjected to predetermined signal processing.

9. The document of claim 1 wherein at least one of the first plural bit and the second plural bits are designed to be lost or to predictably degrade when subjected to predetermined signal processing.

10. The document of claim 1 further comprising a magnetic stripe including information.

11. The document of claim 10 wherein at least one of the steganographically encoded first plural bits of data and the steganographically encoded second plural bits of data cooperate with the magnetic stripe information to verify authenticity of the security document.

12. The document of claim 1, wherein the substrate comprises a first side and a second side, and wherein the first graphic is provided on the first side, and the second graphic is provided on the second side.

13. The document of claim 1, wherein the first plural bits of data and the second plural bits of data cooperate by including at least a portion of redundant data.

14. The document of claim 1, wherein the first plural bits of data and the second plural bits of data cooperate by including corresponding data.

15. The document of claim 14, wherein the corresponding data also corresponds with other data carried by the document.

16. The document of claim 1, wherein at least one of a portion of the first plural bits of data and a portion of the second plural bits of data comprises an issuer identifier.

17. A method of verifying the document of claim 16, comprising: machine-reading at least one of the portion of the first plural bits of data and a portion of the second plural bits of data to obtain the issuer identifier, and handling a remaining portion of at least one of the first plural bits of data and the second plural bits of data in accordance with a predetermined format associated with the issuer identifier.

18. The document of claim 1, wherein the substrate comprises at least one of a laminate layer and a core layer.

19. The document of claim 1, wherein the substrate comprises a laminate layer and a core layer.

20. The document of claim 1, wherein the steganographic encoding comprises digital watermarking.

21. A method to detect swapping of first artwork from a first identification document with second artwork from a second identification document, the swapping resulting in the first artwork being carried on the second identification document instead of the second artwork, wherein the first artwork comprises a first digital watermark embedded therein, and wherein the second identification document comprises a second digital watermark embedded in a first region, said method comprising:

receiving scan data associated with at least a portion of the first artwork and at least a portion of the first region;

analyzing the scan data to detect the first digital watermark and the second digital watermark; and

comparing the first digital watermark with the second digital watermark to detect swapping of the first artwork with the second artwork.

22. The method of claim 21, wherein first digital watermark comprises a first message and the second digital watermark comprises a second message, and wherein said comparing step compares at least a first portion of the first message with at least a first portion of the second message thereby evidencing swapping when the first portion and the second portion do not correspond.

23. The method of claim 22, wherein the first artwork comprises at least a portion of a photographic image of a bearer of the first document, and the second artwork comprises at least a portion of a photographic image an authorized bearer of the second identification document.

24. The method of claim 21, wherein the second artwork comprises a third watermark which is designed to coincide with the second digital watermark.

25. The method of claim 24, wherein the third digital watermark comprises a first message and the second digital watermark comprises a second message, and wherein the first message and the second message comprises redundant or corresponding information.

26. A method to determine whether to authenticate an identification document through a digital watermarking authentication process or through an alternative authentication process, wherein the digital watermark authentication process utilizes at least first and second digital watermarks while the alternative authentication process utilizes bearer or document specific information, and wherein the identification document comprises a detection trigger, said method comprises the steps of:

receiving data corresponding to the detection trigger;

if the received data indicates an expected presence of digital watermarks,

analyzing optical scan data that corresponds to the identification document to attempt to obtain information conveyed by the first and second digital watermarks; and

if the information is obtained, cross-correlating at least some of the information conveyed by the first digital watermark with at least some of the information conveyed by the second digital watermark, and providing a signal corresponding to a result of the cross-correlation of the watermark information; and

if the information is not obtained providing a signal representing that the identification document is considered suspect; and

if the received data indicates an expected absence of digital watermarks,

attempting to obtain the specific information from at least two sources related to the identification document; and

if the specific information is obtained, cross-correlating the specific information, and providing a signal corresponding to a result of the cross-correlation of the specific information; and

if the specific information in not obtained, providing a signal representing that the identification document is suspect.

27. The method of claim 26, wherein the trigger comprises a document issue date.

28. The method of claim 26, wherein the trigger comprises a document expiration date.

29. The method of claim 26, wherein the document comprises a magnetic stripe, and wherein the trigger is stored by the magnetic stripe.

30. The method of claim 26, wherein the document comprises electronic circuitry, and wherein the trigger is stored in the electronic circuitry.

31. The method of claim 26, wherein the document comprises a machine-readable feature, and wherein the trigger is conveyed through the machine-readable feature.

32. The method of claim 31, wherein the machine-readable feature comprises a barcode.

33. The method of claim 26, wherein the trigger comprises a client code.

34. The method of claim 33, wherein the trigger further comprises at least one of a document issue date and a document expiration date.

35. The method of claim 26, wherein the two sources comprise at least two of printed text, magnetic memory, optical memory, electronic circuitry, barcode and a remote database.

36. A security document comprising:

a substrate;

a first graphic carried by the substrate, the first graphic conveying a photographic image to human viewers thereof,

the first graphic being steganographically encoded to convey first plural bits of digital data recoverable by computer analysis of said first graphic;

a second graphic carried by the substrate, the second graphic conveying a visual image to human viewers thereof; and

a detection trigger;

wherein the second graphic is steganographically encoded to convey second plural bits of digital data recoverable by computer analysis of said second graphic,

wherein the steganographically encoded first plural bits of digital data and the steganographically encoded second plural bits of digital data cooperate to verify authenticity of the security document, and

wherein the detection trigger serves to indicate a presence of steganographic encoding.

37. The document of claim 36 wherein the second graphic comprises at least one of a background pattern, a background tint, an image, a graphic design, a photographic image, line-art, a government seal, and an artistic design.

38. The document of claim 37 further comprising text printed on the substrate.

39. The document of claim 38 wherein said first plural bits of digital data and said second plural bits of digital data each correspond to at least a part of said printed text.

40. The document of claim 36 wherein at least one of said first plural bits of digital data and said second plural bits of digital data serves as an index into a registry containing additional information.

41. The document of claim 40 wherein the additional information comprises at least one of a photograph corresponding to the first graphic, biometric information related to a person depicted in the first graphic, and insurance coverage information.

42. The document of claim 36 wherein said steganographic encoding does not visibly interrupt said first or second graphic.

43. The document of claim 36 further comprising steganographic encoding to convey third plural bits, wherein the third plural bits are designed to be lost or to predictably degrade when subjected to predetermined signal processing.

44. The document of claim 36 wherein at least one of the first plural bit and the second plural bits are designed to be lost or to predictably degrade when subjected to predetermined signal processing.

45. The document of claim 36 further comprising at least one of a magnetic stripe and barcode, wherein the at least one of the magnetic stripe and bar code comprises data including the detection trigger.

46. The document of claim 36, wherein the document further comprises text printed thereon and the trigger comprises a predetermined spatial distance between at least one of the first graphic and second graphic and the text.

47. The document of claim 36, wherein the trigger comprises at least one of a color of printed text, a computer-recognizable spatial pattern and an identification document number.

48. The document of claim 36, wherein the trigger comprises artwork.

49. The document of claim 48, wherein the artwork exhibits a predetermined response in a spatial frequency domain.

50. The document of claim 36, wherein the substrate comprises a laminate layer and a substrate layer.

51. The document of claim 50, wherein the trigger comprises the laminate layer.

52. The document of claim 51, wherein the substrate comprises at least one of laser engraving and embossing, and the trigger comprises at least one of the laser engraving and embossing.

53. The document of claim 36, wherein the trigger comprises a predetermined color located in a predetermined position on the document.

54. The document of claim 36, wherein the document comprises text and wherein the trigger comprises a predetermined font in which the text is printed.

55. The document of claim 36, further comprising at least one of a magnetic stripe and bar code, wherein the at least one of the magnetic stripe and barcode comprises information including the detection trigger, wherein the detection trigger comprises a document issue date.

56. The document of claim 36, wherein the trigger comprises a client code.

57. The document of claim 56, wherein the trigger further comprises at least one of a document issue date and a document expiration date.

58. A method of identifying portions of digital data, the digital data corresponding to a printed document, the printed document including first and second different areas conveying first and second different digital watermarks, respectively, wherein the first digital watermark includes a first orientation component and the second digital watermark includes a second orientation component, and wherein the identified portions of the digital data are suspected to include digital watermark data, the method comprising:

segregating the digital data into a plurality of widows;

for each of the plurality of windows, determining an orientation measure;

grouping the windows based on orientation measure; and

selecting at least two of the groups based on at least one of a number of windows assigned to a group and a collective watermark strength for a group, wherein the windows within the selected groups include the portions of the digital data that are suspected to include digital watermark data.

59. The method of claim 58, wherein the two groups are distinguished based on orientation measure.

60. The method of claim 58, wherein the orientation measure comprises a relative scale and a relative rotation.

61. The method of claim 60, wherein the orientation measure further comprises a relative translation.

62. The method of claim 58, further comprising analyzing only the windows within the two groups to detect a watermark message.

63. The method of claim 58, wherein the printed document comprises at least one of an identification document and a financial document.

64. The method of claim 58, wherein the grouping comprises generating a histogram.

65. The method of claim 64, wherein the histogram represents a number of windows over given orientations.

66. The method of claim 64, wherein the histogram identifies predominate watermark orientation components.

67. A method of identifying a first area and a second area of a printed document that are likely to include, respectively, a first digital watermark and a second digital watermark, wherein the first digital watermark includes a first orientation component and the second digital watermark includes a second orientation component, the method comprising:

receiving optically scanned image data that corresponds with at least a portion of the printed document;

segmenting the image data into a plurality of image portions;

determining an orientation measure relative to a predetermined orientation for each of the image portions;

identifying the first area by associating image portions having a first orientation measure; and

identifying the second area by associating image portions having a second orientation measure.

68. The method of claim 67, wherein the first orientation measure and the second orientation measure are each associated with a relatively higher number of image portions when compared to other orientation measures.

69. The method of claim 67, wherein the orientation measure corresponds to a relative scale and a relative rotation.

70. The method of claim 67, wherein the printed document comprises at least one of a financial document and an identification document.

71. The method of claim 67, wherein the first orientation component is embedded so as to represent a first orientation, and wherein the second orientation component is embedded so as to represent a second different orientation.

72. The method of claim 71, wherein the first orientation comprises a first scale, and the second different orientation comprises a second different scale.